UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,567	01/05/2004	Chanwoo Kim	4475-032498	3573

28289 7590 02/11/2009

THE WEBB LAW FIRM, P.C.
700 KOPPERS BUILDING
436 SEVENTH AVENUE
PITTSBURGH, PA 15219

EXAMINER	
SHEPPERD, ERIC W	

ART UNIT	PAPER NUMBER
2456	

MAIL DATE	DELIVERY MODE
02/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/751,567	KIM, CHANWOO	
	Examiner	Art Unit	
	ERIC W. SHEPPERD	2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 January 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to because: In Fig. 1 "Collision decision module" item 46 and "Search list logging & saving module" item 47 are referred to with item numbers 47 and 46 respectively throughout the specification. In Fig. 4, items S87 and S88 are not disclosed in the specification. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. The disclosure is objected to because of the following informalities: Page 5 lines 1-2 "network interface driver module (51)" is shown as "Network interface driver" in Fig. 1 of the drawings. Page 5 line 2 "network interface module (52)" is shown as "Network interface" in Fig. 1 of the drawings. Page 6 line 23 "the search result notification module (43)" is shown as "Detection result notification module" in Fig. 1 of the drawings. Page 6 line 26 "IP collision decision module(45)" is shown as "Collision decision module", item 46 in Fig. 1 of the drawings. Page 6 lines 28-29 the phrase "per IP' MAC address list" is not understood and is believed to be a typographical error. Page 7 line 8 "the" should be capitalized. Page 7 line 24 step "64" is shown as "S64" in Fig. 2 of the drawings. Page 7 line 30 step "65" is shown as "S65" in Fig. 2 of the drawings.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. Claims 1-3 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. As to claim 1, lines 5-6 the limitation "the communication" lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as "communication".

5. As to claim 1, line 9 the limitation “the network” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “a network”.

6. As to claim 1, line 11 the limitation “the devices” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “devices”.

7. As to claim 1, line 22 the limitation “the access” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “access”.

8. As to claim 1, lines 22-23 the limitation “the network access” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “network access”.

9. As to claim 1, line 23 the limitation “the blocked packet” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “the particular packet”.

10. As to claim 1, line 23 the limitation “transmitting an ARP respond packet to the *particular* packet" is vague and indefinite. It is unclear how a packet can be broadcast to another packet. For purposes of applying prior art the limitation has been construed as “transmitting an ARP respond packet *in response* to the *particular* packet”.

11. As to claim 1, lines 27-28 the limitation “the detected collided IP data” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “detected collided IP data”.

12. As to claim1, line 27-28 in the phrase "a search list logging and saving module that internally lists detected collided IP data and periodically it saves in a storage medium" the limitation "it" lacks proper antecedent basis. For purposes of applying prior art the term "it" has been removed, not altering the limitation.

13. As to claim 1, line 30 the limitation "the administrator" lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as "an administrator".

14. As to claim 1, lines 29-30 in the phrase "the detected collided IP data to another system and notifies an administrator of it" the limitation "it" lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as "the detected collided IP data".

15. As to claim 1, line 31 the limitation "the ARP packet" lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as "an ARP packet".

16. As to claim 1, line 32 the limitation "classified into a request packet and a respond packet" is vague and indefinite. It is unclear how an ARP packet can be classified as both a request and a respond packet. For purposes of applying prior art the limitation has been construed as "classified into a request packet *or* a respond packet".

17. As to claim 1, lines 33 (in three separate instances) the limitation "it" lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as "the ARP packet".

18. As to claim 1, lines 33 the limitation “the list” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “a list”.

19. As to claim 1, lines 34 the limitation “the packet’s” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “the ARP packet’s”.

20. As to claim 2, line 3 the limitation “the network” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “a network”.

21. As to claim 2, line 5 the limitation “the filtered ARP packet” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “a filtered ARP packet”.

22. As to claim 2, line 11 the limitation “the ARP respond packets” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “ARP respond packets”.

23. As to claim 2, line 12 the limitation “it” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “the number of ARP respond packets occurring by IP”.

24. As to claim 2, line 13 in the phrase “confirming it as IP collision” the limitation “it” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “the ARP packet”.

25. As to claim 2, line 13 the phrase “adding it to the list” the limitation “it” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “the ARP packet”.

26. As to claim 2, line 13 the phrase “adding it to the list” the limitation “the list” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “a list”.

27. As to claim 3, line 5 the limitation “the filtered ARP packet” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “a filtered ARP packet”.

28. As to claim 3, line 7 the limitation “confirming if an IP address and IP or MAC are included” is vague and indefinite. It is unclear how the “IP address” differs at all from “IP”. For purposes of applying prior art the limitation has been construed as “confirming if an IP address or MAC are included”.

29. As to claim 3, line 8 the limitation “the filtered packet” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “the filtered ARP packet”.

30. As to claim 3, line 9 the limitation “the ARP respond packet” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “an ARP respond packet”.

31. As to claim 3, line 10 the limitation “the policy list” lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as “the block policy list”.

Claim Rejections - 35 USC § 103

32. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

33. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al (US 7,124,197 B2), in view of Thiele et al (US 2005/0050353 A1).

34. As to claim 1, Ocepek substantially discloses a system for detection and blocking of IP collisions, comprising:

a communication interface and communication kernel module ("Operating System" Ocepek Fig. 7, item 104) that provides a communication interface that enables a collided IP detection system to share information with other hosts ("Network Interface Drivers" Ocepek Fig. 7, item 132) and provides a kernel for controlling communication ("Security Module" Ocepek Fig. 7, item 106);

a network interface driver module that is connected with a physical device that is a network interface ("Network Interface Driver" Ocepek fig. 8, item 132 connected to "Network Interface" Ocepek Fig. 8, item 140) and an upper communication module to transmit packets to a network and transmits packets collected in the network to the upper communication module ("Network interface 140 of security device 10 in conjunction with network interface driver 132 provides an interface for transmitting and receiving address resolution requests

and replies to and from network 12" Ocepek column 8 lines 15-20);

a network interface module that is connected to devices connected to the network ("Network Interface" Ocepek Fig. 8, item 140 of "Security Device", item 10 connected to "Network", item 12);

a packet capture driver module that collects all packets detected in the network ("Network Interface driver 132 operates network interface 140 in 'promiscuous' mode" Ocepek Column 9 lines 31-32);

an ARP packet filtering module that filters only ARP packets among the packets being captured from the packet capture driver module ("Detection routing 114 determines if the frame is a "who-has" ARP request" Ocepek column 9 lines 36-37 the *routine singling out ARP requests is a form of filtering*);

an IP collision decision module that determines if the collected packets are collided IP packets ("Upon receipt of the corresponding ARP replies … access monitoring routine determines whether allowed client devices … respond with the same allowed client Mac address 166 found in allowed client list 150" Ocepek column 10 lines 55-60) and, if so, transmits the results to a listing module ("For every MAC address that is not the same or not received, access monitoring routine 120 instructs list control 126 to delete the record from the allowed client list 150" Ocepek column 10 lines 60-62);

an access blocking decision module that notifies an access status if an ARP request packet is included in an access blocking policy list ("Access blocking routine 122 queries list control 126 for records in blocked client list 152" Ocepek column 11 lines 1-2);

an access blocking module that, depending on the access blocking decision module's decision to block access on a particular packet, blocks network access by transmitting an ARP respond packet in response to the particular packet ("For every IP address returned by list control 126 access monitoring routine 120 generates a blocking ARP reply 34 and instructs network interface driver 132 to transmit the blocking ARP replies 34 onto network 12" Ocepek column 11 lines 4-7);

a data storage module that stores information set to operate the collided IP detection system ("Operating system and the routines of security module 106 are run on CPU 134 of security device 10 and may be loaded from secondary memory 136" Ocepek column 8 lines 9-11), a detected collided IP list ("Blocked list" Fig. 8, item 152 *is part of* "Data Structure", item 128 *which is part of the* "Security Module", item 106), and a newly detected host's IP and MAC address lists ("Restricted List" Fig. 8, item 152 *is part of* "Data Structure", item 128 *which is part of the* "Security Module", item 106 *and* "Detection routine then instructs list control to add the IP address of the unknown client device to restricted client list" column 9 lines 46-48);

a search list logging and saving module that internally lists detected collided IP data and periodically saves in a storage medium ("Management of data structure 128 is controlled by list control 126" Ocepek column 8 lines 28-29); and

wherein when an ARP packet is collected from the network, each ARP packet is classified into a request packet ("Detection routine 114 determines if

the frame is a 'who-has' ARP request" Ocepek column 9 lines 36-37) or a respond packet ("Upon receipt of the corresponding ARP reply via network interface driver access blocking routing …" column 11 lines 13-15) after being identified, and the if the ARP packet is a new request packet, the ARP packet is added to a list ("If the IP address is not in access status list … Detection routine then instructs list control 126 to add the IP address of the unknown client device 24 to restricted client list 148" Ocepek column 9 lines 44-48), but if the ARP packet is a respond packet that also exists in input request ARP packet list, the ARP packet's collision is detected and at the same time the ARP packet's access is blocked ("access blocking routine 122 determines whether the client device 24 at the queried IP address responds with the same MAC address as the blocked client MAC address 170 found in blocked client list 152" Ocepek column 11 lines 15-18 *if the address is the same blocking continues, it only stops if the address checked is different*).

Ocepek fails to disclose transmitting the detected collided IP data to another system and notifying an administrator of the detected collided IP data.

Thiele describes a method for detecting unknown computer attacks, by checking packets for known/unknown exploits.

With this in mind, Thiele discloses transmitting the detected collided IP data to another system and notifying an administrator of the detected collided IP data ("program 30 sends the current packet or the entire TCP sequence of related packets which includes the entire TCP sequence of related packets which includes the current packet, as an alert to SOC 40 for further analysis as a fully

filtered, new exploit candidate" Thiele [0027] lines 64-67 *SOC is a* "Security Operations Center" Fig. 1, item 40). It would have been obvious at the time the invention was made to a person of ordinary skill in the art to which said subject matter pertains to combine the method of Thiele with the method of Ocepek as would increase network security by providing the ability to identify new computer viruses, worms, exploitation code or other unwanted intrusions (see Thiele [0011] lines 2-3).

35. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al (US 7,124,197 B2), in view of Matsukawa (US 2001/0017857 A1), in view of Henry et al (US 7,093,030 B1).

36. As to claim 2, Ocepek substantially discloses a method of detecting IP collisions using an IP collision detection system between a client and a server, comprising the steps of:

collecting all packets created by accessing a network ("Network Interface driver 132 operates network interface 140 in 'promiscuous' mode" Ocepek Column 9 lines 31-32);

filtering only ARP packets among the collected packets ("Detection routing 114 determines if the frame is a 'who-has' ARP request" Ocepek column 9 lines 36-37 the *routine singling out ARP requests is a form of filtering*);

determining whether a filtered ARP packet is an ARP request packet or an ARP respond packet ("Upon receipt of the corresponding ARP replies via

network interface driver 132" column 10 lines 55-56);

Ocepek fails to disclose incrementing a count by one for each ARP respond packet; determining if the number of the ARP respond packets occurring exceeds a frequency set within a predefined time out period, and if the number of ARP respond packets occurring by IP exceeds the set frequency, confirming the ARP packet as IP collision and adding the ARP packet to a list; and determining if the number of the ARP respond packets occurring is less than the set frequency, then resetting a counter.

Matsukawa describes a method for detecting duplicate IP addresses using ARP request and respond packets.

With this in mind, Matsukawa discloses incrementing a count by one for each ARP respond packet ("the number of ARP reply packets received is checked" Matsukawa [0043] lines 2-3 *and* "If it is determined that two or more ARP reply packets are received" Matsukawa [0045] lines 1-2 *each reply packet gets counted*); determining if the number of the ARP respond packets occurring exceeds a frequency set within a predefined time out period ("A wait state for an ARP reply packet as a response to the ARP request packet is set with an appropriate period of time" Matsukawa [0039] lines 1-3), and if the number of ARP respond packets occurring by IP exceeds the set frequency ("Two or More" branch of "Number of ARP Reply Packets Received" Matsukawa Fig. 2 item B6), confirming the ARP packet as IP collision ("Determine Detection of IP Address Duplication" Fig. 2, item B8) and adding the ARP packet to a list ("Each input IP address is managed in the form of a list in a database in correspondence with

one of the following assigned states: … "IP address duplication" Matsukawa [0056] lines 1-5); and determining if the number of the ARP respond packets occurring is less than the set frequency ("One" branch of "Number of ARP Reply Packets Received" Matsukawa Fig. 2 item B6). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to combine the duplication detection method of Matsukawa with the method of Ocepek as it provides a substitute method with predictable results, of checking if an IP address is being duplicated.

The above combined art fails to disclose resetting a counter.

Henry describes a network interface driver for processing internetworking protocols for a host computer, independently from the host operating system.

With this in mind, Henry discloses resetting a counter ("Reset Monitoring Counter to Zero" Henry Fig. 5, item 530 *counter is reset after receiving ARP reply* "ARP-Reply Packet Received?" Fig. 5, item 519). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to combine the network interface driver with the method of the above combined art as it would facilitate quicker upgrading of internetworking functions by removing the need to directly modify the IP stack that is built into an operating system (see Henry column 1 lines 20-22).

37. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al (US 7,124,197 B2), in view of Chandra et al (US 7,366,113 B1).

38. As to claim 3, Ocepek substantially discloses a method of blocking collided IP using an IP collision blocking system between a client and a server, comprising the steps of:

collecting all packets transmitted over a network ("Network Interface driver 132 operates network interface 140 in 'promiscuous' mode" Ocepek Column 9 lines 31-32);

filtering only ARP packets among the collected packets ("Detection routing 114 determines if the frame is a 'who-has' ARP request" Ocepek column 9 lines 36-37 the *routine singling out ARP requests is a form of filtering*);

determining whether a filtered ARP packet is an ARP request packet or an ARP respond packet ("Detection routing 114 determines if the frame is a 'who-has' ARP request" Ocepek column 9 lines 36-37);

confirming if an IP address or MAC are included in a block policy list if the filtered ARP packet is an ARP request packet ("the source IP address of the ARP request is compared to the IP addresses found in access status lists 146" Ocepek column 9 lines 37-40);

broadcasting an ARP respond packet to block access, thereby blocking the network access ("blocking ARP replies 34 are broadcast to all devices on network 12" Ocepek column 7 lines 21-22).

Ocepek fails to disclose unicasting an ARP respond packet prior to broadcasting.

Chandra describes a discovery process for mapping all the links in an ad hoc network, including a panic mode for a node that is unable to directly

communicate with its known neighboring nodes.

With this in mind, Chandra discloses unicasting an ARP respond packet prior to broadcasting ("If the node is unable to get a unicast message delivered … it might still be able to get its message sent upstream if it broadcasts it" Chandra column 16 lines 30-34). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to combine the process of Chandra with the method of Ocepek as it increases the ability for nodes of a network to pass messages to each other, strengthening the reliability of the network.

Conclusion

39. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Davis (US 2004/0213220 A1), Massarani (US 6,393,484 B1), Ratcliff et al (US 6,681,258 B1), Schulter et al (US 2002/0156612 A1), Rayes et al (US 2005/0086502 A1), Liston (US 2004/0103314 A1), Rayes et al (US 7,234,163 B1), Nishio (US 7,443,862 B2), Calhoun et al (US 2008/0101283 A1) and Ramachandran et al (US 7,360,245 B1).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ERIC W. SHEPPERD whose telephone number is (571)270-5654. The examiner can normally be reached on Monday - Thursday, Alt. Friday, 7:30 AM - 5PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on (571)272-

3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/E. W. S./
Examiner, Art Unit 2456

/Ashok B. Patel/
Primary Examiner, Art Unit 2456